

30

AFFIDAVIT
PURSUANT TO 37 C.F.R. 1.131

STATE OF CONNECTICUT)
) ss: Stamford
COUNTY OF FAIRFIELD)

1. We, Jay S. Walker, Bruce Schneier, James Jorasch, are the three inventors of the invention described and claimed in pending patent application number 09/112,131, entitled "Method and Apparatus for a Cryptographically Assisted Commercial Network System Designed to Facilitate and Support Expert-Based Commerce."
2. We conceived of and reduced to practice this invention before February 27, 1996 in the United States.
3. The attached Exhibit is a true copy of notes prepared by Jay S. Walker prior to February 27, 1996 that describes the invention.
4. The date deleted from the Exhibit is prior to February 27, 1996.
5. From the time of conception until the filing of the parent application to which the subject application claims priority, we worked diligently with the attorneys at Morgan & Finnegan, L.L.P. to prepare and file application number 08/685,706, the parent of application number 09/112,131.
6. We hereby declare that all statements made herein are of our own knowledge and are true, and that all statements made on information and belief are believed to be true; and further, that these statements are made with the knowledge that willful false statements, and the like so made, are punishable by fine or imprisonment, or both, under Section 1001, Title 18 of the

United States Code, and that such willful false statements may jeopardize the validity of the application identified above or any patent issuing thereon.

7. This document and the document in the Exhibit are provided for use only by the U.S. Patent and Trademark Office for purposes of responding to the Office Action, Paper No. 26, dated December 6, 2000, from the U.S. Patent and Trademark Office with regard to the above-identified patent application. We are not waiving any attorney-client or other privilege associated with, or created as a result of, the parent application, the above-identified patent application, any patent or patent application from which the above-identified patent application claims priority, or any application that claims priority to the above-identified patent application..



Jay S. Walker

Subscribed and sworn to before me this 18th day of December, 2001.


Notary Public

V. S. LELIEVER
NOTARY PUBLIC
MY COMMISSION EXPIRES AUG. 31, 2002

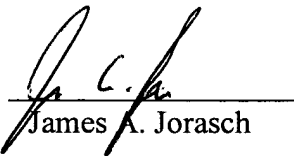
Date my Commission Expires: _____

Bruce Schneier

Subscribed and sworn to before me this _____ day of _____, 2001.

Notary Public

Date my Commission Expires: _____


James A. Jorasch

Subscribed and sworn to before me this 18th day of December, 2001.


Notary Public

V. S. LELIEVER
NOTARY PUBLIC
MY COMMISSION EXPIRES AUG. 31, 2002

Date my Commission Expires: _____

AFFIDAVIT
PURSUANT TO 37 C.F.R. 1.131

STATE OF *Minnesota*
COUNTY OF *Hennepin* ^{ss:}

1. We, Jay S. Walker, Bruce Schneier, James Jorasch, are the three inventors of the invention described and claimed in pending patent application number 09/112,131, entitled "Method and Apparatus for a Cryptographically Assisted Commercial Network System Designed to Facilitate and Support Expert-Based Commerce."
2. We conceived of and reduced to practice this invention before February 27, 1996 in the United States.
3. The attached Exhibit is a true copy of notes prepared by Jay S. Walker prior to February 27, 1996 that describes the invention.
4. The date deleted from the Exhibit is prior to February 27, 1996.
5. From the time of conception until the filing of the parent application to which the subject application claims priority, we worked diligently with the attorneys at Morgan & Finnegan, L.L.P. to prepare and file application number 08/685,706, the parent of application number 09/112,131.
6. We hereby declare that all statements made herein are of our own knowledge and are true, and that all statements made on information and belief are believed to be true; and further, that these statements are made with the knowledge that willful false statements, and the like so made, are punishable by fine or imprisonment, or both, under Section 1001, Title 18 of the

United States Code, and that such willful false statements may jeopardize the validity of the application identified above or any patent issuing thereon.

7. This document and the document in the Exhibit are provided for use only by the U.S. Patent and Trademark Office for purposes of responding to the Office Action, Paper No. 26, dated December 6, 2000, from the U.S. Patent and Trademark Office with regard to the above-identified patent application. We are not waiving any attorney-client or other privilege associated with, or created as a result of, the parent application, the above-identified patent application, any patent or patent application from which the above-identified patent application claims priority, or any application that claims priority to the above-identified patent application..

Jay S. Walker

Subscribed and sworn to before me this _____ day of _____, 2001.

Notary Public

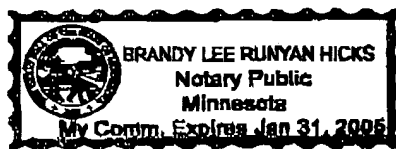
Date my Commission Expires: _____

Bruce Schneier

Subscribed and sworn to before me this 18 day of Dec, 2001.

Notary Public

Date my Commission Expires: Jan 31, 2005



James A. Jorasch

Subscribed and sworn to before me this _____ day of _____, 2001.

Notary Public

Date my Commission Expires: _____

DISCLOSURE: Digital Piecework
Page 1 [REDACTED]

To: [REDACTED]
From: Jay Walker
Re: Disclosure regarding digital piecework

1. What problem are we trying to solve?

How can an effective and efficient system be designed,

1. whereby a first party has a problem requiring human judgement,
(*e.g., the need to grade a test with judgement-related questions.*)
2. and where the problem may be divisible into component parts,
though it is not a requirement that it be so divisible,
(*e.g., the test is composed of individual questions.*)
3. and where those component parts can be electronically distributed to
one or more second parties (a sort of packetizing),
(*e.g., individual questions with the related answers are transmitted
on-line to various graders.*)
4. and whereby one or more second party(s) can make themselves
available for such work on an unscheduled, ad hoc basis.
(*e.g., graders can log on whenever they have time, and any available
work is sent to them.*)
5. and where those second parties can be verified as qualified to address
the component,
(*e.g. each grader is a certified teacher and has known question types
for which he is eligible to serve as a grader.*)
6. and such qualification can be verified by the first party,
(*e.g., each test grader's credentials are listed in a directory.*)
7. but where the identity of the second party may be concealed from the
first party,
(*e.g., the grader's public key is verifiable as proof of their
qualification, but the test-taker does not know their identity.*)

8. and the identity of the first party may be concealed from the second party
(e.g., the grader knows only an identity number or re-mailer address to send back his work.)
9. And the first party may not be able to control which second parties are assigned to address the problem,
(e.g., the questions are distributed to randomly qualified graders.)
10. and where the second party(s) apply their judgement to the component,
(e.g., the grader reviews each question and answer they receive and assigns it a score based on the grader's judgement.)
11. and then transmits their judgement back to the test-taker or an authorized administrative authority,
(e.g., the grader re-transmits their grade back to the sender.)
12. with an irrefutable proof that the second party sent the work,
(e.g., the grader's work is encrypted with the grader's public key.)
13. and with the ability of the first party to ensure the transmission was unaltered,
(e.g., the grader's digital signature insures that the message is unaltered.)
14. and with the ability of a third party to audit the second party's work,
(e.g., if the grader's judgement was wrong, his signature verifies that it was definitely he who made the error.)
15. and where the first party confirms receipt of the second party's work,
(e.g., the test taker provides an irrefutable confirmation receipt to the grader such as a hash of the received document)
16. and thereafter arranges or authorizes payment to the second party, either at a pre-agreed piece rate for such work or an hourly rate.
(e.g. the grader bills the test taker, or an administrative authority, \$2.00 for each question graded)

The Medical Expert Center • An Example

The problem...

I'm arguing with my insurance company about how best to treat my complicated inner ear infection. I want to get three independent opinions as to whether surgery is warranted. (My insurance company refuses to authorize surgery.) I need to have answers no later than the following Friday. I seek only the opinions of doctors who are board-certified inner ear specialists and who have been practicing for five or more years. Each opinion must be at least 200 words in length. If the opinion is anonymous or "unofficial," I'll pay \$100. If the opinion is the physician's "official" signed opinion, I'll pay \$150.

The solution....

I transmit a complete description of my problem, my patient history and digitized x-rays and to the on-line "Medical Expert Center" (MEC). The MEC posts the availability of an expert needed in classification E23 level C or higher for an inner-ear treatment diagnosis with a brief description of the problem. Within 12 hours three doctors have responded. Their qualifications were checked against the expert center database and approved.

The case is transmitted to the doctors over the internet. A piece work value of \$75 is offered for their answer by next wednesday (\$100 is offered if they are willing to provide their "official" opinion). After seeing the case in full, each doctor is given the option to accept or reject the piece work job.

All three accept the job, evaluate the case and transmit their answers back to the MEC signed with their digital signature. All three doctors agree to release their name to me, but only two of the doctors are willing to render an "official" opinion. The MEC forwards all 3 diagnoses to me, whereupon I review them. I have a brief question about one answer. I transmit the question directly to the doctor's e-mail and he responds within a few hours.

I then agree that all three answers met my initial conditions and notify the MEC. My account is billed \$400 for two signed "official" opinions and one unofficial opinion. The doctors who rendered the official opinions receive \$100 each while the third doctor receives \$75.

From the expert's viewpoint:

How can an expert, sitting at home in front of a computer
who wants to earn a few extra dollars,
by selling his/her expert review and opinion,
anonymously (optional),
when he occasionally has the time to do so,
which may become available on a moment's notice,
and cannot predict in advance,

be matched up to people with problems they are willing to pay to solve,
where such problems relate to the expert's area of expertise,
where he can preview the terms of the assignment,
and the price offered for his expertise,
before committing to take the assignment,

and once he accepts the assignment,
can be sure that he'll get paid
so long as he meets the terms of the assignment.

From the questioner's viewpoint

How can a questioner with a specific problem
who needs the problem answered,
by one *or more* qualified experts,
whom the questioner may not know how to find,
any who may remain choose to remain anonymous,
as long as the questioner can independently verify,
that the expert is qualified to answer the problem,
at the price the questioner is willing to pay,
with the level of detail the questioner sets forth in advance,
no later than the deadline set forth by the questioner,
where the questioner has the ability to accept or reject the answer,
and the questioner may ask the expert to provide clarification if needed.

Sample Digital Piecework Assignments

1. I want a draft of an academic paper on quantum mechanics reviewed anonymously by three qualified academics not located in the U.S. The reviews, which are due by July 15, should be at least 500 words and must explain the three points with which the reviewers most agree and disagree.
2. I am a businessman in the steel salvage business with a question as to how to handle a personnel problem. I would like my question answered by a personnel professional at a Fortune 1000 company who is not in the steel business and who has dealt with the same or similar problem at least five times in their own company and can thus give me a range of possible results based on their own experience. I am willing to pay \$100 for answers of at least 250 words. Anonymity is acceptable, but I will pay an extra \$100 if the professional is identified to me and I am allowed to call the professional in their off hours.
3. I am attorney who is seeking other businesses who have had a problem with the XYZ company's plastic products. I will pay \$50 for each documented example of problems you have experienced first hand, up to a maximum of 100 cases.
4. I am looking to decode a hieroglyphic unearthed on a site in Israel. I will pay \$50 for each solution of at least 10 words, and \$500 for the complete solution. Answers will be accepted from 4 candidates who send me their credentials.
5. I am looking to find John X. Smith, last known address 100 York Street, Anytown, USA. (Description to follow). I will pay \$500 to the first person who provides me with a verified place of employment of this person.
6. I have 1,000 english literature final exams that I need graded. Each exam is composed of 10 short essay questions. Tests and answers can be e-mailed to you in groups of twenty exams, and must be graded and returned via e-mail no later than June 10, 1996. I will pay \$2.00 per graded exam. Graders must be practicing english teachers at the college level and follow the grading guidelines which will be sent to you.
7. I'm seeking to hire a qualified structural engineer for a two-week assignment performing a weight-load analysis for various wooden bridges.
8. To all people who have eaten at my restaurant, I will pay you \$5.00 for a 100 word description of how to improve my service or my menu. (limit 50 people)

2. What is the prior art?

3. What are the shortcomings of the prior art?